

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF OREGON**

**UNITED STATES OF AMERICA,**

v.

**ANDRE EUGENE SHAW,**

Defendant.

Case No. 3:15-cr-00227-SI

**OPINION AND ORDER**

Billy J. Williams, United States Attorney, and Gary Y. Sussman, Assistant United States Attorney, United States Attorney's Office for the District of Oregon, 1000 S.W. Third Avenue, Suite 600, Portland, Oregon 97204. Of Attorneys for United States of America.

Richard L. McBreen III, OWENS & MCBREEN, P.C., 319 S.W. Washington Street, Suite 614, Portland, OR 97204. Of Attorneys for Defendant Andre Eugene Shaw.

**Michael H. Simon, District Judge.**

Defendant Andre Eugene Shaw ("Defendant") was indicted in this criminal action for possession of false identification cards and supplies for making false identification cards, among other charges. Before the Court is Defendant's Motion to Compel Informant's Identity and Defendant's Motion to Compel Disclosure of Mirror Images of Computer Hard Drives. For the reasons that follow, the Court defers ruling on Defendant's Motion to Compel Informant's

Identify (Dkt. 22) pending an *in camera* hearing. Defendant's Motion to Compel Disclosure of Mirror Images of Computer Hard Drives (Dkt. 23) is DENIED.

## **BACKGROUND**

A search warrant for Defendant's home was signed on December 17, 2014. The warrant authorized the seizure of multiple items including records, documents, or contraband relating to the production, transportation, distribution, and possession of child pornography; selling and buying of children; blackmail; interstate communication of threats; receiving proceeds of extortion; and fraud and related activity in connection with computers and identification documents. The Government executed the warrant on December 18, 2014. Law enforcement officials seized, among other things, multiple firearms, silencers, ammunition, computers and other electronics, false identification cards, and supplies for making false identification cards.

On June 17, 2015, a federal grand jury returned an Indictment charging Defendant with one count of possession of an unregistered firearm, a violation of 26 U.S.C. § 5861(d); one count of possession of unregistered silencers, a violation of 26 U.S.C. § 5861(d); one count of possession with intent to use unlawfully five or more false identification documents, a violation of 18 U.S.C. § 1028(a)(3), (b)(2); and one count of possession of a document-making implement or authentication feature with intent to produce a false identification document, in violation of 18 U.S.C. § 1028(a)(5), (b)(1).

## **DISCUSSION**

### **A. Motion to Compel Informant's Identity**

#### **1. Legal Standard**

"The government has a limited privilege to withhold an informant's identity." *United States v. Henderson*, 241 F.3d 638, 645 (9th Cir. 2001) (citing *Roviaro v. United States*, 353 U.S. 53, 59-61 (1957)). "This privilege serves several important law enforcement objectives,

including encouraging citizens to supply the government with information concerning crimes.”

*Id.* The defendant bears the burden of demonstrating the need for disclosure. *United States v. Williams*, 898 F.2d 1400, 1402 (9th Cir. 1990). To obtain disclosure, the defendant “must show more than a ‘mere suspicion’ that the informant has information which will prove ‘relevant and helpful’ to his defense, or that it will be essential to a fair trial.” *Henderson*, 241 F.3d at 645 (quoting *United States v. Amador-Galvan*, 9 F.3d 1414, 1417 (9th Cir. 1993)). Whenever the defendant makes a “‘minimal threshold showing’ that disclosure would be relevant to at least one defense,” the court must hold an *in camera* hearing on disclosure. *Id.* (quoting *United States v. Spires*, 3 F.3d 1234, 1238 (9th Cir. 1993)).

In determining whether disclosure is warranted, the court must balance: (1) the extent to which disclosure would be relevant and helpful to the defendant’s case; and (2) the government’s interest in protecting the identity of a particular informant. *Spires*, 3 F.3d at 1238. The court “must consider ‘the public interest in protecting the flow of information against the individual’s right to prepare his defense.’” *Id.* (quoting *Roviaro*, 353 U.S. at 62).

## 2. Argument

Defendant moves to compel the Government to produce the identity of a confidential informant (“S1”). Defendant asserts that S1’s identity is relevant to Defendant’s guilt or innocence, and that the disclosure would be helpful to his defense and essential to the fair determination of his case. Defendant additionally requests the “informant file,” including:

1. The name and date of birth of S1;
2. Copies of any agreement between S1 and the Government;
3. Copies of documents relating to S1’s personal and criminal history;
4. How much money S1 is paid for his information and activities;
5. Any instructions to S1 regarding his work with law enforcement;

6. Any documentation of past contacts S1 has had with Defendant;
7. Whether law enforcement has declined to prosecute or arrest S1 in exchange for his work and other benefits of the informant's cooperation.

Defendant asserts that disclosure of information in the "informant file" is constitutionally required because it is essential to determining Defendant's guilt or innocence in this case.

According to the parties, in Special Agent Charles Dodsworth's ("S/A Dodsworth") affidavit in support of the December 17, 2014 search warrant for Defendant's residence, S/A Dodsworth describes information that S1, who is involved in the production and distribution of child pornography, provided to law enforcement investigators. S1 told law enforcement investigators that someone using the screen name "Reedemer" was blackmailing him online. "Reedemer" was aware of S1's child pornography activities and threatened to expose those activities unless S1 paid him. S1 reported that "Reedemer" also used him as a conduit to receive blackmail payments from other "Reedemer" victims. According to S1, the blackmail payments were sent to S1 in the form of wire money transfers. S1 would then send the money to a person in Oregon who S1 knew as "Joe." In order to make the anonymous financial transactions, S1 received false identification cards from "Joe." According to S1, "Reedemer" provided the false identification cards to "Joe." Law enforcement investigators assert that "Joe Stanis" is an alias used by Defendant.

The Government additionally asserts that "Reedemer" demanded photographs of S1's daughter. S1 was instructed to turn his daughter over to "Joe," which he did on two separate occasions. It was S1's understanding that "Joe," or others that "Joe" knew, would take sexually explicit photographs of S1's daughter. S1 was instructed to buy costumes, props, and a camera for the photography sessions, which S1 provided to "Joe" and "Joe" returned to S1. Investigators later found Defendant's palm print on a box containing the costumes and camera.

Defendant argues that the disclosure of S1's identity is necessary because S1 was a participant in the alleged criminal conduct, as well as a witness. For example, S1 may have information that could establish whether the false identification cards were made by Defendant or by another individual. Additionally, S1 may have information regarding whether Defendant had knowledge that what he was transporting to S1 were false identification cards. Thus, Defendant argues that S1 has information "'relevant and helpful' to his defense, or that will be essential to a fair trial." *Henderson*, 241 F.3d at 645 (quoting *Amador-Galvan*, 9 F.3d at 1417).

The Government responds that it anticipates seeking additional charges against Defendant stemming from his alleged role in blackmailing and extorting other individuals, as well as his alleged role in the production of child pornography involving S1's daughter. The Government asserts that S1 will be a direct victim in at least some of these counts and a percipient witness to others. Thus, the Government states that if a grand jury returns a superseding indictment, the Government will provide Defendant with S1's identity, although not with his date of birth, and with discovery of statements made by and evidence obtained from S1. The Government represents that it will provide Defendant with a copy of any plea or cooperation agreement reached with S1, as well as S1's criminal history.<sup>1</sup>

The Government, however, does not provide any date by which they intend to seek additional grand jury proceedings. Additionally, the Government asserts that it will disclose S1's identity only if grand jury returns a superseding indictment. Thus, any voluntary disclosure by the Government is speculative at this time.

Two of the four charges against Defendant relate to the alleged possession and creation of false identification cards. According to S1, "Reedemer" provided Defendant with false

---

<sup>1</sup> Because S1 was not a paid informant, the Government asserts that there are no records of payment for information or activities.

identification cards, which Defendant in turn provided to S1. Thus, S1 may have information that could establish whether the false identification cards were made by Defendant or by another individual, and that could establish whether Defendant had knowledge that what he was transporting were false identification cards. Accordingly, Court finds that Defendant has made a “‘minimal threshold showing’ that disclosure would be relevant to at least one [of his] defense[s].”<sup>2</sup> *Henderson*, 241 F.3d at 645 (quoting *Spires*, 3 F.3d 1238). Thus, the Court is required to hold an *in camera* hearing to determine whether disclosure of S1’s identity to Defendant is warranted. *Id.*

## **B. Motion to Compel Disclosure of Mirror Images of Computer Hard Drives**

### **1. Legal Standard**

FRCP 16(a)(1)(E)(i) provides that a criminal defendant is entitled to discovery of documents and tangible things that are within the government’s possession, custody, or control if the requested information is “material to preparing the defense.” Information is in the government’s possession if the prosecutor “‘has knowledge of and access to the documents sought by the defendant.’” *United States v. Stever*, 603 F.3d 747, 752 (9th Cir. 2010) (quoting *United States v. Santiago*, 46 F.3d 885, 893 (9th Cir. 1995)). In order to obtain discovery under FRCP 16, a defendant must make a prima facie showing of materiality. *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990). “Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense.” *Id.*

---

<sup>2</sup> The Court notes that the Government makes no argument to the contrary.

## 2. Argument

Defendant moves to compel the production of mirror images of hard drives seized during the December 18, 2014 search of his home. Defendant asserts that information contained on the hard drives is material to preparing his defense against the charges of alleged possession and creation of false identification cards. That is, Defendant represents that the hard drives contain information for relevant files including the dates of their creation, modification, and access, and that Defendant will use this information to counter prosecution arguments regarding the creation of the allegedly false identification cards and Defendant's intent in their creation and purported use. Defendant additionally asserts that that information from the hard drives is material as it may help him establish that the skills used in the commission of the alleged offenses were not sophisticated. The Court finds that these facts satisfy the prima facie showing of materiality required under FRCP 16. *See Mandel*, 914 F.2d at 1219.

The Government responds that the hard drives are exempt from FRCP 16 disclosure under the Adam Walsh Child Protection and Safety Act (the "Act"), 18 U.S.C. § 3509. The Act provides, in relevant part:

(1) In any criminal proceeding, any property or material that constitutes child pornography . . . shall remain in the care, custody, and control of either the Government or the court.

(2)(A) Notwithstanding Rule 16 of the Federal Rules of Criminal Procedure, a court shall deny, in any criminal proceeding, any request by the defendant to copy, photograph, duplicate, or otherwise reproduce any property or material that constitutes child pornography . . . so long as the Government makes the property or material reasonably available to the defendant.

(B) For the purposes of subparagraph (A), property or material shall be deemed to be reasonably available to the defendant if the Government provides ample opportunity for inspection, viewing, and examination at a Government facility of the property or material by the defendant, his or her attorney, and any individual

the defendant may seek to qualify to furnish expert testimony at trial.

18 U.S.C. § 3509(m). The Government asserts that each of the hard drives that Defendant seeks copies of is encrypted and that Defendant has refused to decrypt any of them.<sup>3</sup> Thus, although the Government has a valid warrant to search the hard drives, it has been unable to access the data located on the drives. As a result, the Government does not know whether the hard drives actually contain child pornography. Nonetheless, the Government argues that the hard drives are exempt from disclosure under the Act.

Defendant recognizes that courts have found a sufficient basis to apply the Act where “there is an indictment [charging a defendant with possession of child pornography because] a federal grand jury has already found probable cause to believe that the material at issue is child pornography.” *United States v. Battaglia*, 2007 WL 1831108, at \*2 (N.D. Ohio June 25, 2007). Here, however, Defendant has not been indicted on any charges relating to child pornography. The Government does not provide the Court with any authority for the proposition that material may be protected under the Act even though there has been no determination—preliminary or otherwise—that the material is or may be child pornography.

The Government asserts that Defendant should be required to either decrypt the hard drives or forego their disclosure under FRCP 16. To do so, however, may be to require Defendant to choose between giving up his Fifth Amendment right against self-incrimination and giving up his right to discovery under the Federal Rules of Criminal Procedure. The Court will

---

<sup>3</sup> As the Government notes, courts are reluctant to order a defendant to decrypt an encrypted hard drive because it may implicate the defendant’s Fifth Amendment right against self-incrimination. *See In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1341 (11th Cir. 2012) (holding that the defendant’s “decryption and production of the hard drives’ contents would trigger Fifth Amendment protection because it would be testimonial, and that such protection would extend to the Government’s use of the drives’ contents.”).

not order Defendant to make that choice and thus declines to order Defendant to decrypt the hard drives.

The Government adds in its response to Defendant's motion that the Government will provide Defendant's counsel and his expert "reasonable access to, and an ample opportunity to examine, any drive or device that *does* contain child pornography at a government facility, just as it does in every child pornography case." Dkt. 24 at 9 (emphasis in original). Here, as discussed, it is unknown whether the hard drives contain child pornography. Defendant has not made a showing, however, of why the opportunity to access and examine the hard drives at a government facility would be insufficient.<sup>4</sup> Accordingly, Defendant's Motion to Compel Disclosure of Mirror Images of Computer Hard Drives is denied, but the Government must permit Defendant's counsel and expert reasonable access to and an ample opportunity to examine the hard drives that are the subject of this motion at an appropriate government facility.<sup>5</sup>

### CONCLUSION

The Court defers ruling on Defendant's Motion to Compel Informant's Identity (Dkt. 22) pending an *in camera* hearing on disclosure of the confidential informant's identity. Defendant's Motion to Compel Disclosure of Mirror Images of Computer Hard Drives (Dkt. 23) is DENIED. It is further ordered that the parties shall file within 30 days a status report updating the Court on these issues.

---

<sup>4</sup> Defendant has leave to renew his Motion to Compel Disclosure of Mirror Images of Computer Hard Drives if he believes that he is able to make such a showing.

<sup>5</sup> The Court reiterates that it is not ordering Defendant to decrypt the hard drives and make them accessible to the Government.

**IT IS SO ORDERED.**

DATED this 1st day of March, 2016.

/s/ Michael H. Simon  
Michael H. Simon  
United States District Judge